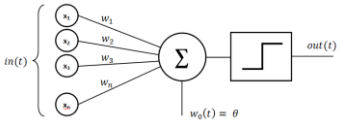
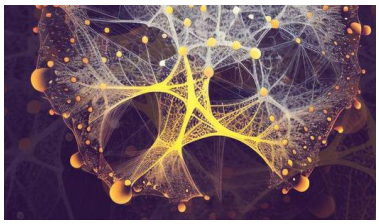
Digitalisaation teknologiakohtaisia aiheita

Tekoäly

Tässä osiossa käyn lyhyesti lävitse tekoälyn perusteita ja merkitystä liiketoiminnassa yleensä, sekä esimerkkejä toimialakohtaisista kyberuhista.

Tekoälyn pitkät juuret





- **Alunperin 1950-luvulta (esim. perceptron)**
- **Nykyisin: generatiiviset verkot, kielimallit, ym.**
- **“Vanhat mallit” yhä elossa**
  - Erit. teollisuudessa
  - AI käyttöön enemmän ongelman kuin tavan vuoksi
- **Vanhojen mallien etuja**
  - Selitettävyys
  - Vähemmän herkkiä kyberhyökkäyksille

2

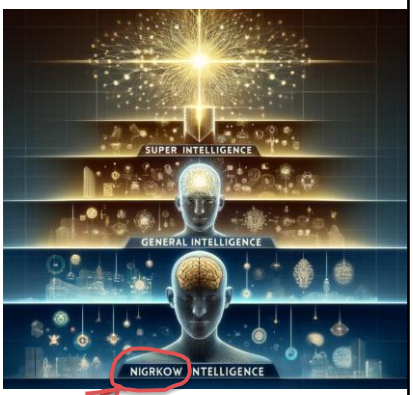
Tekoälyllä on pitkä historia. 1950-luvulla pyrittiin matkimaan yksittäisten neuronien toimintaa matemaattisella mallilla (perceptronilla). Laskentatehon ja mallien kehittyessä nykyään puhutaan generatiivisista verkoista, syväoppimisesta ja kielimalleista muun muassa.

“Vanhat mallit”, joita on nykyisten konvolutiivisten verkkojen ja transformereiden lisäksi lukuisia luokkia, ovat edelleen käytössä varsinkin järjestelmissä, joilla on pitkä elinkaari. Tuolloin oli yleistä, että tekoälyjärjestelmiä otettiin käyttöön, koska jokin tietty AI-tyyppi tiedettiin hyväksi ratkomaan juuri tietynlaista ongelmaa, jota organisaatiossa esiintyi. Nykyisin tekoälyä otetaan helposti käyttöön pelkästään itsensä vuoksi ja toivotaan, että siitä seuraa liiketoimintaa tai prosessien optimoimista.

Vanhojen mallien etuna kyberturvallisuuden kannalta on edelleen parempi selitettävyys ja yksinkertaisuutensa vuoksi pienempi hyökkäyspinta-ala kybervaikuttamiselle.

Tekoälyn kyvykkyyksistä

- **Tekoäly on pääasiassa tarkoitettu luokitteluun ja ennakointiin**
  - ... mutta tämän voi viedä hyvin pitkälle
  - Luokkien lukumäärä (ja luominen)
- **Oppiminen ilman valvontaa**
- **Oppiminen ja yleistäminen**
  - Varo ylioppimista (overfitting)
- **Tuntemattomien riippuvuuksien etsiminen datasta**
  - “Lisää vain kerroksia”
- **Kuinka Big Datan saa käyttöön**



“Narrow”

3

Tekoälylle on kirjallisuudessa esitetty kolme hyvin karkeajakoista luokkaa: kapea, yleinen ja super-tekoäly. Yleisenä tasona pidetään ihmisen älykkyyttä. Nykyisten järjestelmien uskotaan olevan vielä kuitenkin kapealla alueella (vaikkakin kielimallit teknisesti ottaen läpäisevät nykyään Turingin testin).

Kapea tekoäly on tarkoitettu luokitteluun ja ennakointiin. Kummatkin voi kuitenkin automatisoida nykyisin hyvin pitkälle, ja järjestelmät kykenevät käsittelemään valtavaa määriä luokkia, luomaan uusia luokkia, ennakoimaan tarkasti ja pitkälle (esimerkiksi kielimallit ennakoivat hyvinkin pitkälle uskottavaa tekstiä) ja löytämään tuntemattomia riipuvuuksia datasta.

Nykyisten tekoälyjärjestelmien vahvuus onkin siinä, että dataa ei tarvitse esikäsitellä enää niin paljon, jos järjestelmään vain lisää vähän tehoa (kerrosten määrää kasvattamalla), ja sinne voi johdon näkökulmasta vain kaataa yrityksen datan ja sieltä alkaa löytymään uusia innovaatioita ja tapoja parantaa liiketoimintaa.

Ihan näin suoraviivaista nykyistenkään tekoälyjärjestelmien käyttö ei tietenkään ole, vaan niiden virittely vaatii edelleen paljon asiantuntemusta.

Tekoälyn rajoituksista

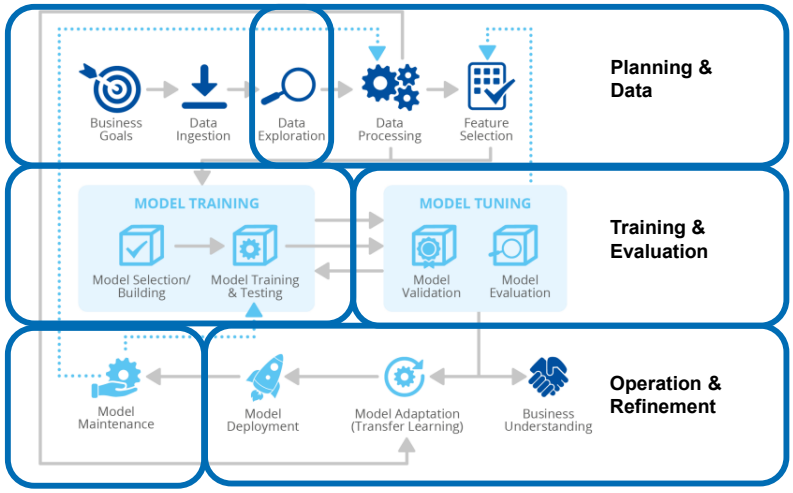
- **Yleistäminen <> tarkkuus**
- **Yleistäminen vain kapeassa merkityksessä (toimialan sisällä)**
- **Massiiviset datavaatimukset**
- **Ei täydellistä riippumattomuutta**
  - Data tarvitsee huolellista valmistelua
  - Mallit vaativat ylläpitoa operoinnin aikana
- **Liiketoiminnan tavoite: “160 kg tekoälyä = €€€”, mutta...**
  - Yhdistäminen liiketoimintaprosesseihin haastavaa
  - Operoinnin aikaista hienosäätöä ja optimointia tarvitaan
  - Liiketoimintaprosessin muuttuminen → uudelleenopetus
  - Sopivatko liiketoimintaprosessisi tekoälyn käyttöön?
  - Henkilöstön uudelleenkoulutus

4

Yleistävät tekoälymallit eivät ole kovin tarkkoja. Tämä ei sinänsä ole uutta, mutta edelleenkin esimerkiksi ainoa syy sille, että ChatGPT osaa matematiikkaa, on se, että siihen on integroitu Python-tulkki, ja ChatGPT pystyy tunnistamaan matemaattiset lausekkeet. Tekoäly pystyy kyllä luomaan uusia luokkia ja etsimään aiemmin tuntemattomia syy-yhteyksiä datasta, mutta vain käsittelemiensä datatyyppien rajoissa.

Mitä monimutkaisempi malli, sitä enemmän data sen kouluttaminen vaatii. Mikäli yrityksen bisnesprosesseja kyetään automaattisesti monitoroimaan ja tuloksia digitalisoimaan AI:n oppimateriaaliksi, sitä paremmin sen voi olettaa toimivan. Toisaalta, jos kysymys on ihmisten käyttäytymisen ennakoinnista (kuten kaupan alalla) tai logistiikkaverkon toiminnasta, datan kerääminen ei enää olekaan niin yksinkertaista.

Tekoälyn elinkaari (ENISA)



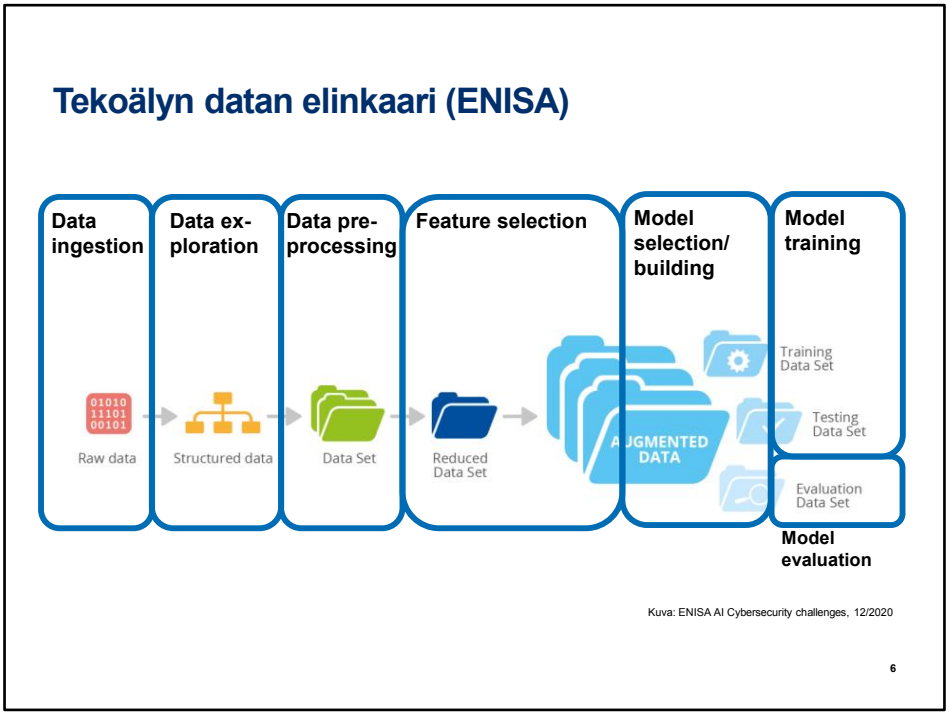
Kuva: ENISA AI Cybersecurity challenges, 12/2020

5

On hyvä muistaa, että tekoälyn kehittäminen ja käyttöönotto on omanlaisensa kehitysprosessi, eikä kehittäminen pysähdy vielä operointivaiheessakaan.

Tekoälyn on erittäin riippuvaista datasta, ja koulutusdataan onkin kiinnitettävä erityistä huomiota sen valinnasta aina esikäsittelyn loppuun asti. Mallin kouluttaminenkaan ei tapahdu yhdessä vaiheessa, vaan sisältää useamman testaus- ja validointivaiheen.

Tekoälyn erikoisuutena on nk. transfer learning. Tämä tarkoittaa toisen samantyyppisen mallin optimointien siirtämistä operoitavan mallin käyttöön parantamaan sen suorituskykyä. Jossain mielessä analoginen ohjelmistokirjastojen käytölle, mutta rajatuimmin käyttökohtein ja tiukemmin soveltuvuusehdoin.



Tekoälyn kehittäminen operatiiviseen valmiuteen vaatii paljon data, sen käyttäminen vaatii data, itse asiassa koko tekoälyjärjestelmä *on* data.

Tämän vuoksi tekoälyjärjestelmissä yleisesti ottaen datallakin on oma elinkaarensa. Elinkaari sisältää useita vaiheita, ja datasta on tärkeää jättää osa “käyttämättä” kussakin vaiheessa seuraavan vaiheen tarkastusta varten. Jopa operointivaiheeseen jätetään pieni, kriittisen tärkeä datasetti, jonka perusteella järjestelmän toiminta voidaan keskeyttää, jos ko. datasetin kanssa ei toimita oikein.

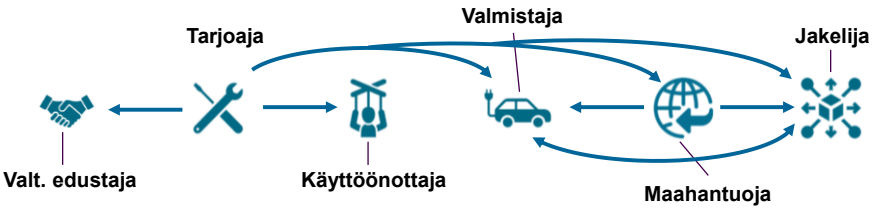
Datan elinkaaren vaiheet ovat:

- Raakadatan hankinta ja valinta. Tässä vaiheessa on hyvä tarkastaa, ettei raakadatassa tule ilmenemään tilastollisia vinoumia, esimerkiksi toimipisteiden välisten prosessien tai pohjapiirustusten erilaisuuksien vuoksi.
- Datan muuttaminen rakenteiseksi (exploration) tarkoittaa datatyyppien tunnistamista ja erilaisten tilastollisten tunnuslukujen arviointia
- Datan esiprosessoinnissa puhdistetaan, yhdistellään ja muunnetaan dataa formaatista toiseen.
- Piirrevalinnan vaiheessa tehdään juuri kyseisellä tekoäly-

/syväoppimismallille tarvittava esikäsittely.

Itse mallin rakentamisen ja testaamisen kanssa erotetaan vielä erillisiä datasettejä alkane testausdatasta ja päätyen evaluoinnin ja operatiivisen kriittisen testidatan joukkoihin.

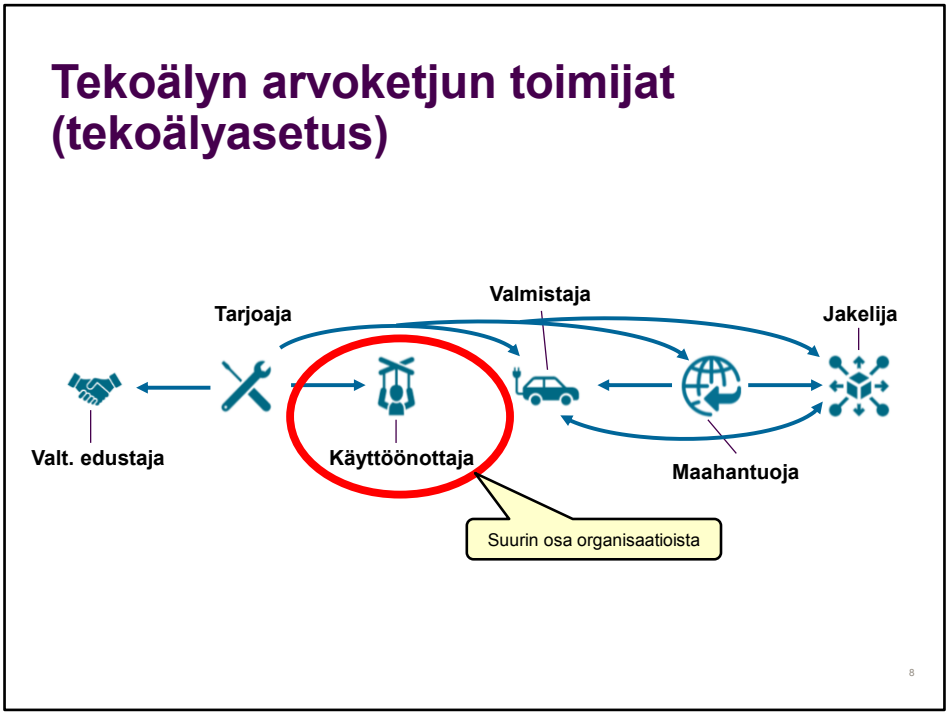
Tekoälyn arvoketjun toimijat (tekoälyasetus)



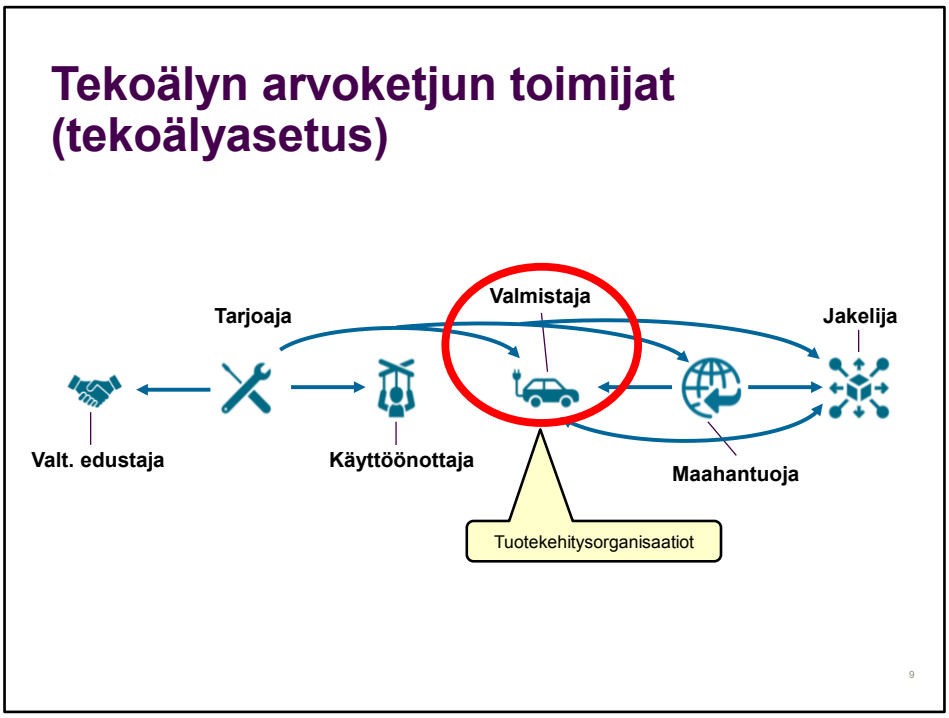
7

Tekoälyn arvoketjun mukaiset toimijan EU tekoälyasetuksen mukaan ovat:

- Tarjoaja / Provider: taho, joka kehittää tekoälyjärjestelmiä käyttöön (näitä on myös pienimuotoisia ja arvoketjussa eteenpäin tarjontaa tekeviä tahoja=
- Käyttöönottaja / Deployer: tahot jotka käyttävät tekoälyjärjestelmiä työnsä puolesta (harrastuskäyttö erikseen)
- Valmistaja / Manufacturer: taho, joka tekee muita tuotteita (esim. autoja), joihin soveltaa tai lisensoi tekoälyjärjestelmiä
- Jakelija / Distributor: tahot, jotka tuovat tekoälyjärjestelmiä EU-markkinoille joko omansa tai alihankkijansa tavaramerkin alla
- Maahantuoja / Importer: kuten jakelija, mutta tuo tekoälyjärjestelmiä EU:n markkinoille EU:n ulkopuolelta EU:n ulkopuolisen tavaramerkin alla
- Valtuutettu edustaja / Representative: EU:ssa oleva taho, jonka jokin taho on palkannut auttamaan oman tuotteensa markkinoille saattamiseen EU:n tekoälyasetuksen mukaisesti.



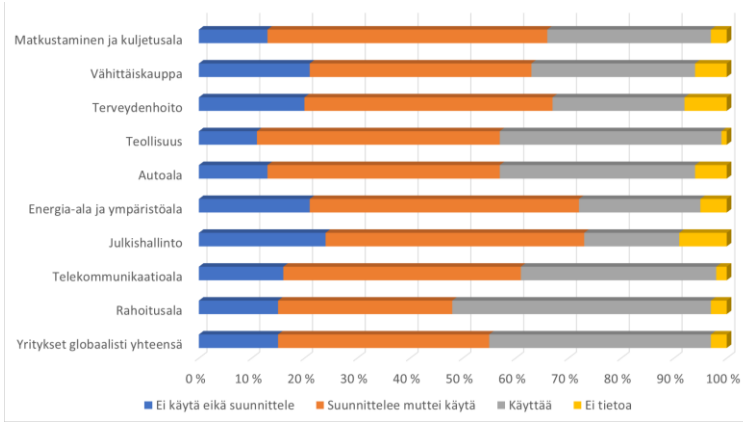
Suurin osa organisaatioista kuuluu arvoketjussa käyttöönottajiin. Huom. tekoälyasetus asettaa velvollisuuksia organisaatiolle suojella työntekijöitään ja ottaa vastuu tekoälyjärjestelmien asetuksen mukaisesta käytöstä.



Tuotekehitysorganisaatiot, jotka käyttävät tekoälyjärjestelmiä uusien tuotteiden valmistamiseen kuuluvat arvoketjussa valmistajiin.

Tekoälyn käyttö liiketoiminnassa toimialueittain

Käyttääkö organisaatiosi, tai suunnitteleeko käyttävänsä tekoälyä osana liiketoimintaprosessejaan ja digitalisaatiota?



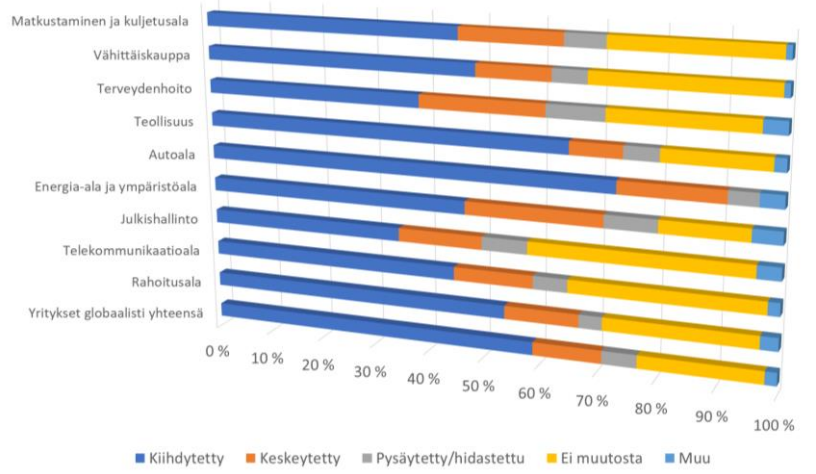
Lähde: IBM Global AI Adoption index 2023

Kuinka yleistä tekoälyn käyttö sitten liiketoiminnassa on? Onko se merkittävää liiketoiminnan digitalisaatiossa? IBM julkaisee vuosittain tutkimuksia asiasta.

Käyttö vaihtelee toimialoittain, mutta epäluuloisimmillakin toimialoilla jo viidennes käyttää tekoälyä, ja joillakin alueilla vain 10%:lla ei ole mitään suunnitelmia sisällyttää tekoälyä toimintoihinsa. Tämän kurssin toimialueista vähittäismyynti (retail) edustaa melko lailla keskiarvoa ja kuljetuslogistiikka on murroksessa ottamassa tekoälyä runsaasti käyttöön.

Tekoälyn käyttöönoton nopeus toimialueittain

"*Mikä on yrityksenne tekoälyn käyttöönoton / kehityksen tilanne viimeisen 24kk aikana?*"
[niiden joukosta, jotka ovat ilmoittaneet ottavansa AI:tä käyttöön liiketoiminnassaan]



Lähde: IBM Global AI Adoption index 2023

Lähestulkoon kaikki toimialat ovat n. vuoden sisällä kiihdyttäneet tekoälyn käyttöönottoa, erityisesti autoala ja valmistusteollisuus. Vähittäiskaupasta ja kuljetuslogistiikastakin n. puolet kiihdyttävät tekoälyn käyttöönottoa.

Tekoälyn käyttöalueet toimialueittain

	Yritykset yleensä	Väh.kauppa	Kuljetusala
IT-prosessien automatisointi	33 %	27 %	21 %
Turvallisuus, ja uhkien havaitseminen	26 %	23 %	19 %
Tekoälyn avulla tehtävä valvonta ja johtaminen	25 %	24 %	14 %
Dokumenttivirtojen valvonta ja tilanneymm.	24 %	21 %	11 %
Liiketoiminta-analytiikka ja BI	24 %	14 %	28 %
Asiakkaiden/työntek. itsepalv. automatisointi	23 %	21 %	28 %
Liiketoimintaprosessien automatisointi	22 %	16 %	11 %
Verkostoprosessien automatisointi	22 %	19 %	16 %
Digitaalinen työvoima	22 %	20 %	9 %
Petoksen havainnointi	22 %	20 %	21 %
Markkinointi ja myynti	22 %	20 %	35 %
Tiedonhaku ja -louhinta	21 %	14 %	14 %
HR	19 %	16 %	19 %
Rahoitussuunnittelu ja -analyysi	18 %	13 %	16 %
Ennakoiva päätöksenteko	18 %	16 %	19 %
IoT-sensoridatan analyysi	18 %	15 %	9 %
Toimitusketjujen tilannekuva	18 %	19 %	18 %
Ohjelmistokoodin tuottaminen	17 %	14 %	12 %
Visuaalinen tunnistaminen	16 %	16 %	14 %
Kestävä kehitys	13 %	11 %	7 %
Riskianalyysi ympäristölle	12 %	11 %	11 %
Terveydenhuollon diagnostiikka	11 %	4 %	11 %
Ei mikään edellisistä	4 %	10 %	2 %
Muu	0 %	0 %	2 %

Lähde: IBM Global AI Adoption index 2023

Tekoälyn oma kyberturvallisuus

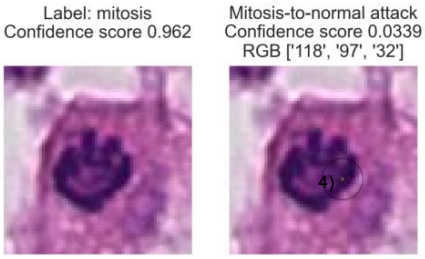
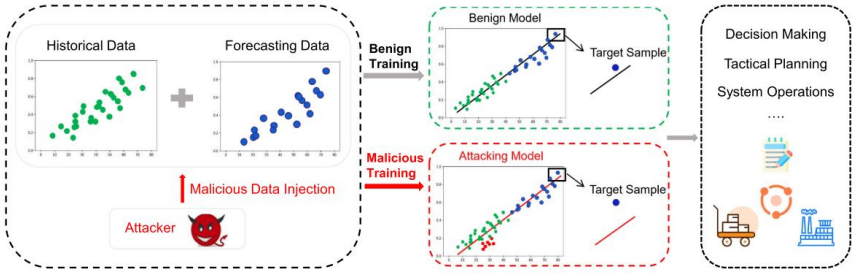


Figure 1: An image recovered using a new model inversion attack (left) and a training set image of the victim (right).

Tekoäly on itsessäänkin altis kyberhyökkäyksille. Nykyiset deep learning –verkot ovat niin kompleksisia, että vähän sopivasti aiotusta sivussa olevilla herätteillä saadaan aivan toisenlaisia tuloksia. Pääasialliset termit ovat ohittaminen/ohitus, eli evasion, jossa käytössä olevalle järjestelmälle esitetään hiukan muunnettuja syötteitä, ja tekoäly kuvittelee kyseessä olevan jotakin aivan muuta. Myrkytyshyökkäyksessä tekoälyn opetusprosessiin syötetään vinoutunutta dataa, jolloin oikeillakin syötteillä mennään vinoon.
Kolmas pääluokka on (yleensä luottamuksellisen) opetusdatan varastaminen, kuten esimerkiksi yritys uuttaa ChatGPT:ltä pomminvalmistusohjeita.

Toimialuekohtaisia hyökkäyksiä AI:tä vastaan

- Hyökkääjän tavoite:
  - Tietyn tuotteen kysynnän väärinarviointi
  - Esim. aliarvioitu kysyntä rokotteille
  - Esim. aliarvioitu tarve pakettien varastotilalle
- Lähtökohta:
  - Hyökkääjä kykenee arvioimaan opetusdatan todennäköisyysjakauman havainnoimalla materiaalivirtoja
  - Hyökkääjä muodostaa myrkytettyä opetusdataa ja syöttää sen opetusvaiheeseen
- Piiloutuminen:
  - Muiden tuotteiden kysynnän ennakointi normaalissa



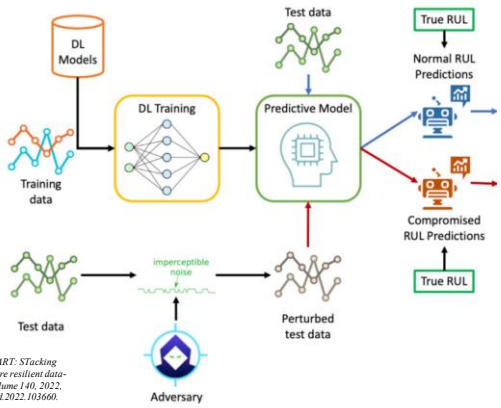
From: Chen, Jian & Gao, Yuan & Shan, Jinyong& Peng, Kai & Wang, Chen & Jiang, Hongbo. (2023). Manipulating Supply Chain Demand Forecasting With Targeted Poisoning Attacks. 19. 1803-1818. 10.1109/TI.2022.3175958.

Tekoälyä vastaan tehdyt kyberhyökkäykset tuntuvat kovin kaukaisilta, ennen kuin ymmärretään, että haavoittuvia tekoälyjärjestelmiä on jo monella toimialalla: esimerkiksi kysynnän ennakointiin tarkoitettuja järjestelmiä käytetään niin kaupan, huolinnan kuin varastologistiikankin alalla.

Tämä kyseinen hyökkäys on vasta kokeellinen, mutta kuitenkin täysin mahdollinen.

Toimialuekohtaisia hyökkäyksiä AI:tä vastaan

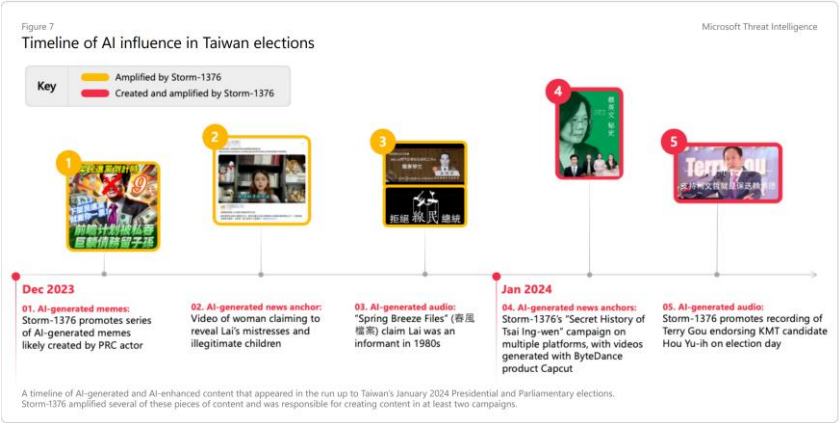
- Hyökkääjän tavoite:
  - Täydellisen satunnainen komponentin hajoamisiän (Remaining Useful Life, RUL) väärinarviointi
  - → Rikkinäisiä osia, turhaa kunnossa olevien komponenttien korvaamista, epäluottamus RUL:iin
- Lähtökohta:
  - Hyökkääjä kykenee lisäämään komponenttien sensoreihin huolellisesti valmisteltua “kohinaa”
- Tulos:
  - Jopa 120x virheet estimoinnissa
- Piiloutuminen:
  - “Kohinan” itseisarvo hyvin pientä



From: *Onat Gungor, Tajana Rosing, Baris Aksanli,STEWART: STacking Ensemble for White-Box AdversaRial Attacks Towards more resilient data-driven predictive maintenance, Computers in Industry, Volume 140, 2022, 103660,ISSN 0166-3615,https://doi.org/10.1016/j.compind.2022.103660.*

Komponenttien vikaantumista halutaan kyetä ennakoimaan monissa pitkälle automatisoiduissa fyysisissä järjestelmissä, kuten varastologistiikan robotiikassa ja kuljetuslogistiikan kalustoissa.

Toimialuekohtaista AI:n väärinkäyttöä



Tekoälyn käyttö media-alalla on erityisen voimakasta ja sen väärinkäyttö tuottaa haastaviakin ongelmia. Pääasiallinen uhka on tekoälyn kautta eri tavoin tuotettu disinformaatio, mukaanlukien, mutta ei rajoittuen nk. deep fake-tekniikoihin.

Eräs esimerkki, joka kiinnostaa niin yhteiskunnan turvallisuusviranomaisia kuin uutistoimituksiakin, on vaalivaikuttaminen disinformaatiolla. Tästä saatiin kokeiluluontoinen esimerkki Taiwanin presidentinvaaleissa tänä (armon) vuonna 2024. CCP, eli Kiinan kommunistinen puolue antoi tehtäväksi DragonBridge-nimiselle uhkatoimijalle sabotoida vaaleja. Vaikuttaminen ei ollut kovin laajaa ja määrätietoista, todennäköisesti tässä kokeiltiin eri menetelmien toimivuutta ja tehokkuutta.

Käytettyjä taktiikoita olivat mm.

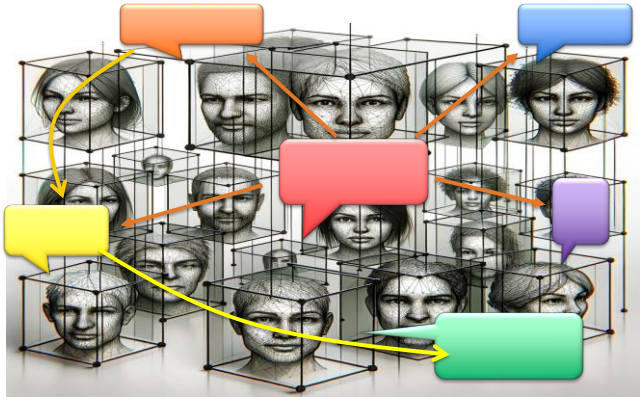
- Kuva- ja tekstipohjaisten meemien massiivinen tuotanto some-alustoille
- AI:llä tehdyt uutisankkurit (huom. Bytedancen CapCut-työkalu)
- DeepVoicella tehdyt rikoskehystykset
- Deepvoicella oikean videon päälle puhuttu ääni

Toimialuekohtaista AI:n väärinkäyttöä

Tätä kirjoitettaessa deep fakellä ei kovin helposti voida tuottaa aidon näköisiä videoita, ja kuvissakin on useimmiten helppo tunnistettavuus. Toisaalta erilaiset hybriditekniikat, kuten väärennetyn äänen lisääminen oikeaan videoon, tai aidon kuvan osan manipulointi tekoälyllä voi tuottaa uskottavankin oloista materiaalia. Esimerkiksi tässä väitetty pommi-isku Pentagonin viereen. Tausta on aito, mutta savu on tehty AI:llä.

Deepfake tulevaisuudessa?

- **Deepfake + ChatGPT?**
- **Deepfaken + 5G?**



18

Rajoittamattomien ChatGPT:n kaltaisten työkalujen käyttö yhdessä deepfaken kanssa voi johtaa hyvin helposti tuotettaviin disinformaatiokampanjoihin, esimerkiksi “Tuota 500 profiilin laajuinen rasistinen chat-kampanja IG:hen, Fortnite-kanaviin ja Snapchatiin seuraavilla kielillä. Käytä näitä tarkempia aiheita...”. Kriittinen massa nykyisillä some-algoritmeilla voi olla hyvinkin helppoa tuottaa.

Deepfake käyttää pääasiassa multi- ja anycast-tyyppisiä leviämismekanismeja. TV ja radio ovat (ainakin toistaiseksi) kriittisempiä mediankulutuksen ja levittämisen suhteen. Toisaalta uudet tulevat teknologiat, kuten 5G, nojaavat yhä enemmän multi- ja anycast-tyylisiin vertaisverkon kaltaisiin lähetyksiin broadcastin jäädessä vähemmälle. Tämä lisää deepfaken vaikuttavuutta.

VAHTI: tekoälyn huoneentaulu johdolle

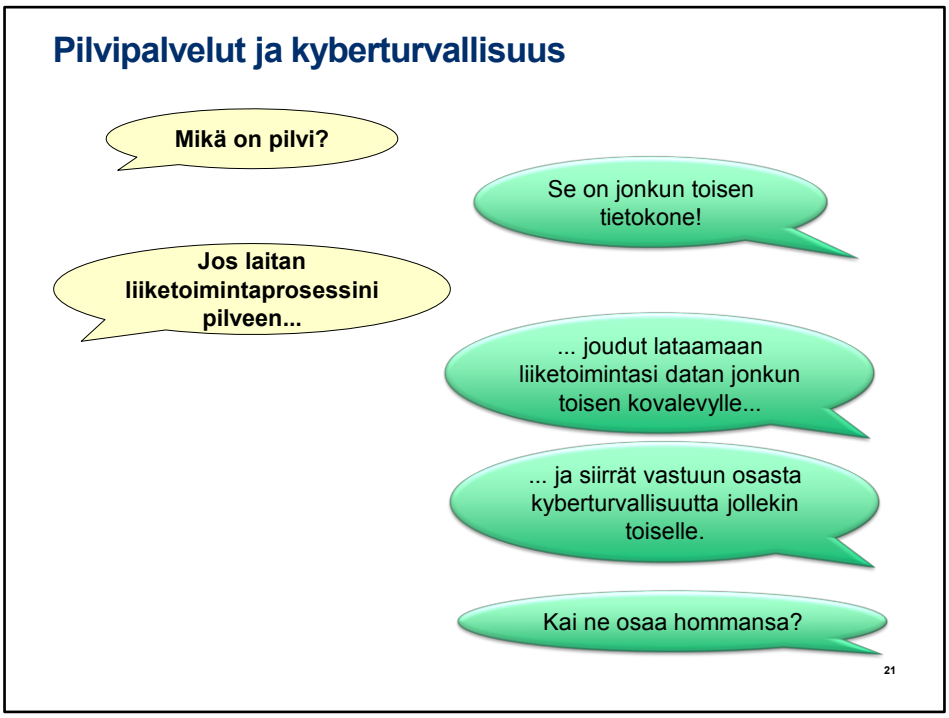
- **Kouluta tekoälyn perusteet johdolle**
- **Valmistele visiot, strategiat, suunnitelmat ja politiikat**
- **Määrittele ja budjetoi tekoälyyn liittyvät vastuut, roolit ja resurssit**
- **Sido AI:n käyttö ja kehittäminen organisaation riskienhallintaan**
- **Suunnittele ja toteuta muutosjohtaminen ja –viestintä, kun uusia AI-liitännäisiä kokonaisuuksia otetaan käyttöön**
- **Varmista, että organisaatiossa tunnetaan AI:n ohjeistus**

https://dvv.fi/digiturvajulkaisut, v.2.0, 12.12.2023

Mitä johto voi sitten tehdä tekoälyn mukanaan tuomille kyberuhkille? Yksi tiivistys on tässä, digiviraston ja VAHTIn ylläpitämät kyberturvallisuuden eri alueiden “huoneentaulut”.

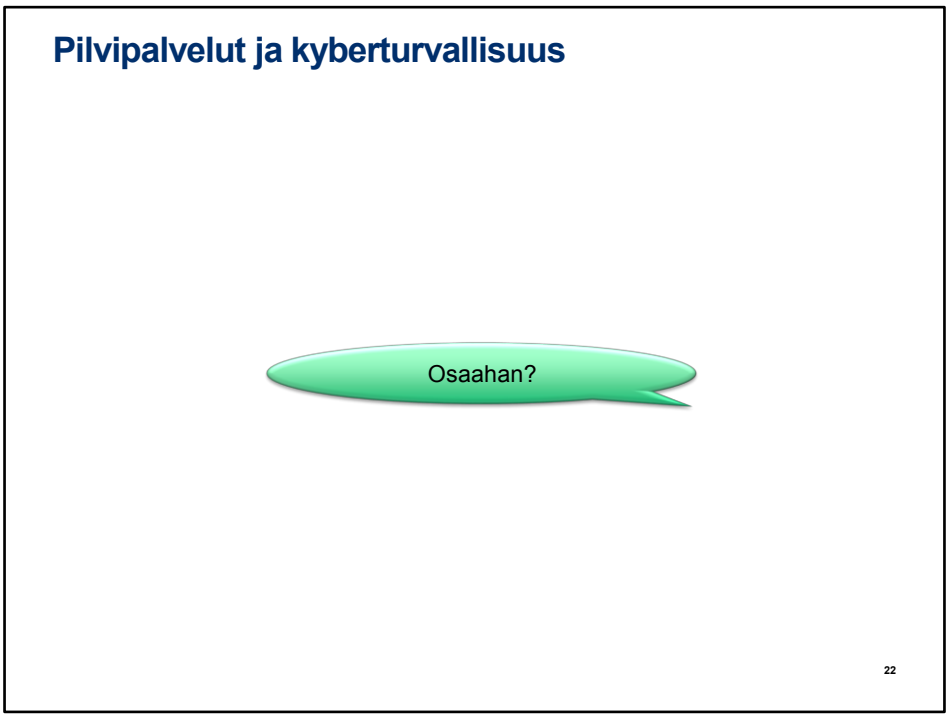
Digitalisaation teknologiakohtaisia aiheita

Pilviteknologiat

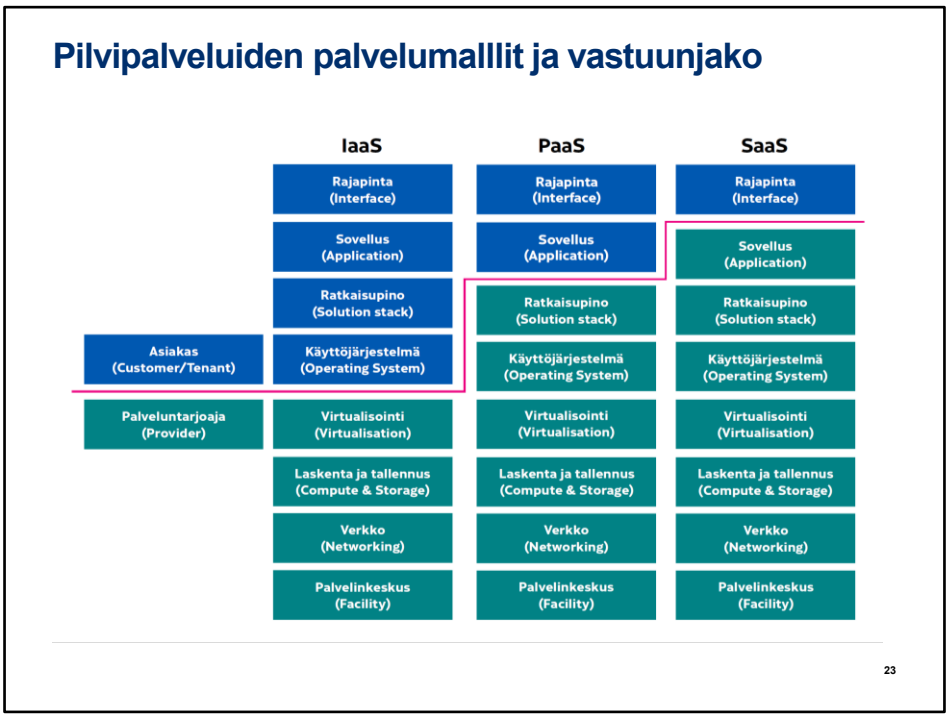


“Pilvipalvelut” nousivat n. 2000-luvun taitteessa hype-käyrälle.
Mallissa uutta ei ollut niinkään se, että laskentaa ulkoistettiin toisille tietokoneille, vaan se, että rajapintaa fyysisestä (client-server) arkkitehtuurista nostettiin useampien välikerrosten kautta 1) riippumattomaksi osoitteistuksesta ja sijainnista 2) liiketoimintaprosessien tasolle
Pilvipalvelut voidaan nähdä digitaalisena palvelujen ulkoistamisena.
Palvelujen ulkoistaminen digitaalisesti tarkoittaa kuitenkin...
... että ulkoistuksen hoitavalle taholle siirtyy väkisinkin jonkin verran yritykselle tärkeää dataa. Tällöin palveluntarjoajalle siirtyy myös vastuuta kyseisen datan ja prosessien turvallisuusvastuista, eritoten kyberturvallisuudesta.

Oletuksena on luonnollisesti tällöin, että sekä pilvipalvelun käyttäjä että tarjoaja tunnistavat roolinsa sekä vastuunsa, ja osaavat hoitaa riskienhallinnan sekä kyberturvallisuuden kuten asiaan kuuluu.



Pilvipalveluita on kuitenkin monenlaisia, ja vastuunkin rajat kulkevat usein eri kohdissa. Näihin on onneksi kuitenkin olemassa jo suosituksia ja luokituksia, jotka on kyettävä tunnistamaan osana johtamisprosessia ja riskienhallintaa.



Pilvipalvelut on jaettu useaan kerrokseen lähtien itse palvelintiloista ja laitteistosta sovelluksiin ja sovellusrajapintoihin. Pilvipalveluiden logiikkaan kuuluu se, että samaa kapasiteettia tulee voida käyttää useammalle asiakkaalle joustavasti, eli yhden asiakkaan käyttäessä vähemmän resursseja samalle palvelimelle voidaan ottaa enemmän asiakkaita tai vapauttaa resursseja niitä enemmän tarvitsevalle. Tämä hoidetaan nk. virtualisointikerroksella, ja käytännössä melko harvoin on mahdollista vuokrata palveluja tämän kerroksen alapuolelta.

Virtualisointikerroksen yläpuolelta sen sijaan on eri vaihtoehtoja asettaa palvelurajapinta riippuen asiakkaan tahtotilasta ja osaamisesta järjestellä itse omaa teknologiaansa. Tärkeimmät tasot ovat (NIST SP 800-145:n mukaan):

- Infrastructure as a service (IaaS). IaaS-palvelumallissa tarjoaja antaa asiakkaalle käyttöön pelkkää laskentakapasiteettia, mutta asiakas tuo käyttöjärjestelmästä lähtien omat järjestelmänsä ajoon palveluntarjoajalle
- Platform-as-a-Service (PaaS): tässä mallissa asiakas tuo yksittäisen ohjelmiston, esim. jokin ERP-ohjelmisto palveluntarjoaja ympäristöön johonkin kohtaan ratkaisupinoa (eri sovellukset tarvitsevat eri tason palveluita, eikä pelkkä käyttöjärjestelmä välttämättä riitä).
- Software-as-a-Service (SaaS). Mallissa palveluntarjoaja hallinnoi myös

ohjelmistoja, ja asiakas syöttää sinne pelkän datan.

Vastuiden jakautuminen noudattaa palvelumallia, mutta myös palvelumallin sisällä on useita eri tapoja jakaa vastuut.

Pilvipalveluiden omistajuuden mukaan yleisimmät toteutusmallit voidaan jakaa yksityiseen pilveen (private cloud), yhdistelmäpilveen (hybrid cloud), ja julkiseen pilveen (public cloud). Muut toteutusmallit, esimerkiksi jonkin eri toimijoista koostuvan yhteisön yhteisöpilvet (community/government cloud), ovat yleensä arvioitavissa yleisimpien toteutusmallien pohjustamana.

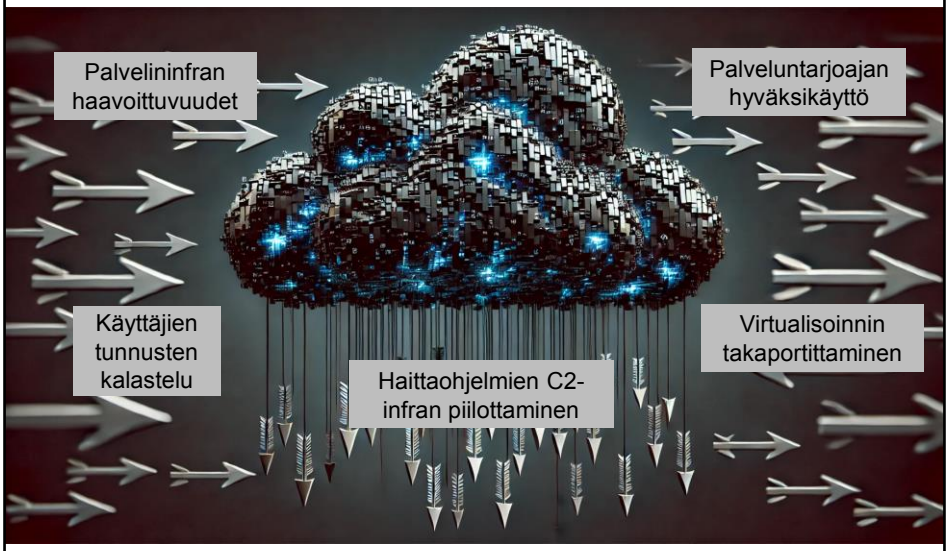
Yksityisellä pilvellä tarkoitetaan palvelua, joka tuotetaan vain palvelua käyttävälle organisaatiolle. Palvelua voidaan tuottaa joko palveluntarjoajan tai/ja käyttäjäorganisaation konesaleista. Yksityisen pilven tyypillisenä vahvuutena on pilvipalveluinfrastruktuurin sekä siinä käsiteltävien tietojen fyysisen ja loogisen tason luotettava erottelu muista tietojenkäsittely-ympäristöistä, käyttäjäorganisaatioista ja ulkoisista toimijoista. Yksityisellä pilvellä pystytään toteuttamaan tyypillisesti korkeamman turvatason palveluja, kuin muilla toteutusmalleilla.

Julkisella pilvellä tarkoitetaan palvelua, joka on julkisesti tarjolla ja hankittavissa kenen tahansa toimesta. Palvelua tuotetaan lähes poikkeuksetta palveluntarjoajan konesaleista. Julkisessa pilvessä pilvipalveluinfrastruktuuriin sekä siinä käsiteltäviin tietoihin kohdistuu yksityistä pilveä laajempi hyökkäyspinta-ala muun muassa palvelun muiden

käyttäjien tai ulkoisten toimijoiden kautta.

Yhdistelmäpilvellä tarkoitetaan palvelua, jossa yhdistetään yksityinen pilvi sekä julkinen pilvi yhdeksi palvelukokonaisuudeksi. Esimerkiksi organisaation omassa konesalissa ajettavaa yksityistä pilveä voidaan täydentää julkisesta pilvestä hankittavilla palveluilla. Toteutuva turvataso riippuu tyypillisesti siitä, mitä tietoja on mahdollista siirtyä julkisen pilven puolelle, ja miten turvallisuus on järjestetty pilvitoteutusten rajapinnoissa.

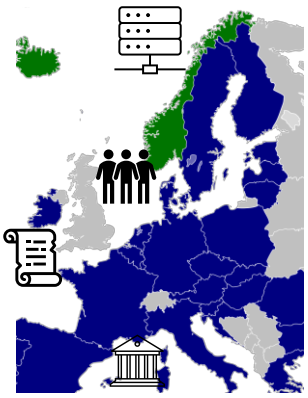
Pilvipalveluiden kyberuhkia



24

Pilven kyberturvallisuuden tekijöitä: sijainti

- **Pilvipalvelun komponenttien hajautuminen**
  - Konesalien sijainti
  - Palveluntuottajayrityksen kotipaikka
  - Ylläpitohenkilöstön sijainti
  - Ei-toiminnallisten tietojen (esim. lokitiedot ja asiakastieto) sijainti



25

Nykyisin melkein kaikki liiketoiminnan IT-toiminnot ovat pilvessä. Kyberturvallisuuden ja riskienhallinnan suositukset onkin rakennettu tietoisina tästä. Pilvipalveluiden riskit eivät enää niinkään tule teknologiasta (vaikka eivät nekään katoa, esim. palvelunestohyökkäykset ja murtautuminen pilven kontista toiseen), vaan hallinnollisista ja juridisista tekijöistä.

Pilvipalvelun kyberturvallisuuden hallittavuuden kannalta on tärkeää tietää, minkä lainsäädännön alla mikäkin palvelun osa toimii, nämä nimittäin eivät useinkaan ole samassa paikassa. Erityisesti tulee erottaa konesalien, ylläpitohenkilöstön ja ei-toiminnallisten tietojen sijainti, sekä lisäksi itse palveluntuottajayrityksen kotipaikka.

Pilven kyberturvallisuuden ohjeistusta

26

Pilvipalvelu-spesifistä kyberturvallisuusohjeistusta on runsaasti saatavilla. Suomessakin viranomainen on ottanut kantaa valtionhallinnon pilvipalveluiden käyttöön, ja näitä voidaan käyttää myös muiden organisaatioiden pilviturvallisuuden hallintaan.

Valtionhallinnon näkökulma on, että pilveen voi sopivin turvamekanismein laittaa henkilötietoja, SALPID- ja korkeintaan TLIV-tietoa.

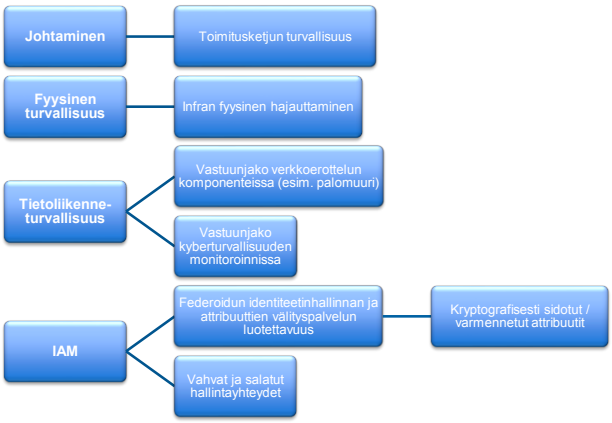
Tarkemmin pilviturvallisuutta tarkastellaan nk. PiTuKrissä, joka on virallisesti tarkoitettu viranomaisten salassa pidettävän tiedon kyberturvallisuuden arviointiin (maks. TLIV/RESTRICTED). Käyttö muissa organisaatioissa onnistuu esim. riskienhallinnan sisäisenä tarkastuslistana.

PiTuKri tarkastelualueet

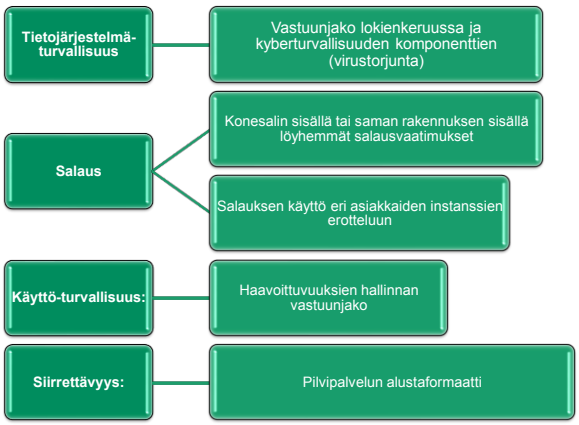
Alue	Sisältö
Esiehdot	Dokumentointivaatimukset ja lainsäädäntökohtaisten reunaehtojen tarkastus. Viranomaisen kannalta sensitiivinen tieto palveluntarjoajineen oltava kotimaassa.
Turvallisuusjohtaminen	Turvallisuusperiaatteet, organisaation sisäiset vastuut, riskienhallinta, häiriöiden hallinta, jatkuvuudenhallinta, suojattavien kohteiden luokittelu ja merkintä, vaatimuksenmukaisuus ja tietosuoja. Velvoitteita myös palveluntarjoajien sopimustekniseen sitouttamiseen.
Henkilöstöturvallisuus	Työsuhteen elinkaaren huomioiminen, henkilöstön luotettavuuden arviointi, NDAt, turvallisuustietoisuus, tiedonsaantitarpeet ja tehtävien erottelu
Fyysinen turvallisuus	Monitasoinen suojaaminen (defence-in-depth), sensitiivisen ICT-infran tilojen suojaus, kulkuoikeuksien hallinta, vierailukäytännöt, jatkuvuudenhallinta
Tietoliikenneturvallisuus	Verkon rakenne (erottelumahdollisuudet), verkkohyökkäyksiä vastaan suojautuminen
IAM	Käyttöoikeushallinta, käyttäjätunnistus, hallintayhteydet
Tietojärjestelmäturvallisuus	Jäljitettävyys ja havainnointikyky, järjestelmäkovennus, tiedon erottelu, haittaohjelmasuojaus, suojattavien kohteiden siirtäminen ja poistaminen
Salaus	Salauskäytännöt ja avaintenhallinta, salaus fyysisesti suojatun alueen ulko-/sisäpuolella
Käyttöturvallisuus	Järjestelmäkuvauksien olemassaolo, suorituskyvyn hallinta, varmistus- ja palautusprosessit, haavoittuvuuksien hallinta
Siirrettävyys ja yhteensopivuus	APIen julkistaminen, ohjelmistojen alustaformaatti (kuten Kubernetes), standardoidut protokollat ja salausmenetelmät, aineistojen tuhoamisvalmiudet
Muutostenhallinta	Muutostenhallinta ja järjestelmäkehitys

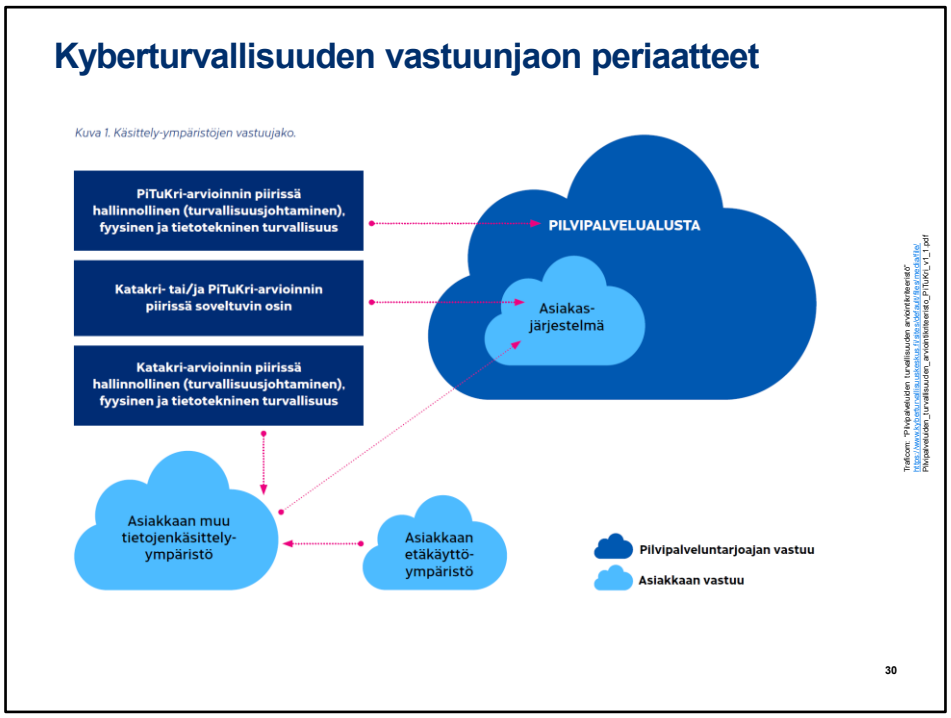
27

Pilvipalvelukeskeiset turvallisuusalueet (PiTuKRI perusteella)



Pilvipalvelukeskeiset turvallisuusalueet (PiTuKRI perusteella)





Kyberturvallisuuden vastuiden jako asiakkaan ja palveluntarjoajan välillä noudattelee yksinkertaisia periaatteita: asiakkaan etäkäyttöympäristö ja pilvipalvelusta riippumaton tietojenkäsittely-ympäristö ovat pelkästään asiakkaan vastuulla (ja näitä koskevat myös muut kuin pilviturvallisuuden ohjeistukset).

Pilvipalvelualustalla olevat järjestelmät ovat palvelumallin osoittaman vastuujaon mukaisesti joko asiakkaan tai palveluntarjoajan vastuulla. Näitä koskeva ohjeistus määräytyy alustan hallinnan perusteella.

Vastuukysymysten jakautuminen tarkastelualueittain

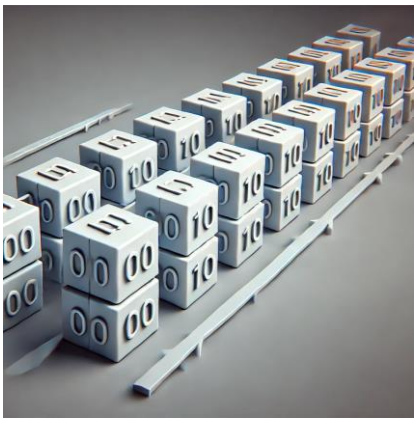
Alue	IaaS		PaaS		SaaS	
Esiehdot	0	2	0	2	0	2
Turvallisuusjohtaminen	7	1	7	1	5	3
Henkilöstöturvallisuus	5	-	5	-	5	-
Fyysinen turvallisuus	-	-	-	-	-	-
Tietoliikenneturvallisuus	2	-	2	-	-	-
IAM	3	-	3	-	1	2
Tietojärjestelmäturvallisuus	4	1	2	3	-	-
Salaus	3	-	3	-	0	3
Käyttöturvallisuus	5	1	4	1	1	-
Siirrettävyys ja yhteensopivuus	2	2	2	2	0	3
Muutostenhallinta	2	-	1	1	1	-

31

Digitalisaation teknologiakohtaisia aiheita

Hajautetut ja digitaaliset tilikirjat

Mitä ovat lohkoketjut



- **Lohko = tietue**
- **Lohkoketju = toisiinsa loogisesti ketjutettuja lohkoja**
  - Tarkistettavissa: lohkojen muuttaminen ja siirtely
- **Hajautetut lohkoketjut**
- **Gävlen lohkoketju = Haminan lohkoketju?**

  → Konsensusprotokolla
- **Monia konsensusprotokollia**
  - Laskentatehoon perustuvat (proof-of-work, esim. bitcoin)
  - Omistukseen perustuvat (proof-of-stake, esim. Ethereum 2.0)
  - Viralliseen määräysvaltaan perustuvat (Proof-of-Authority, esim. JP Morgan)

Lohkoketjut ovat teknologialtaan suoraviivaisia ymmärtää: yksi lohko koostuu jostakin tietueesta, eli tietojen kokonaisuudesta, jotka käyttäjä määrittää; esimerkiksi postipaketin tunnistetiedot, tai vaikkapa postilähetyksen yhden vaiheen tiedot.

Joskus käsiteltävät tiedot muodostavat peräkkäin Olevia kokonaisuuksia, kuten vaikkapa postilähetyksen eri vaiheet, jossa myöhempi vaihe pitää kyetä sitomaan aikaisempaan vaiheeseen luotettavasti. Esimerkiksi, kun paketin tulisi saapua jakelukeskukseen lentokoneesta purkamisen jälkeen, tulee yleensä vähintään tehdä erilaisia kuittauksia. Lisäksi, mikäli paketti ei saavukaan, tulee kyetä jäljittämään tapahtumaketjun “lohkoja” taaksepäin.

Lohkon sitominen toiseen tapahtuu nk. kryptografisin, eli salausteknisin keinoin: on mahdollista lisätä kuhunkin lohkoon tarkistetietoja, joita on lähes mahdotonta väärentää. Jokaisen lohkon kohdalla voidaan siis tarkistaa edellisen lohkon tietojen perusteella, että kukaan ei ole muuttanut tai siirrellyt aiempia lohkoja keskenään.

(NIIN: se “krypto” tulee itse asiassa myös lohkoketjuissa käytetyistä tietoturvatekniikoista, eikä Bitcoinista tai sanaristikoista)

Hajautetut tilikirjat

- **Hajautettu tilikirja (Distributed Ledger Technology, DLT)**
- **Lohkoketju – tilikirjat**
- **Hyperledger – tilikirjat**
  - R3 Corda, Hyperledger-Fabric
- **DLT:n etuja**
  - Käyttövarmuus
  - Tehokkuus
  - Automatisointi
  - Läpinäkyvyys → seuranta ja mittaaminen
- **DLT:n käyttötapoja:**
  - Rahoitusala ja maksuliikenteen seuranta
  - Toimitusketjun seuranta
  - Identiteetin hajautettu hallinta
  - Liikkuvan työvoiman hallinta
  - Automatisoidut “piensopimukset”

34

“Tilikirjalla” tarkoitetaan tässä yhteydessä yleistä kirjanpitoa siitä, mitä on sovittu, mitä mikäkin maksaa, kuka maksoi ja minne, milloin tavara lähti, minne se saapui yms. Tilikirja voi sisältää myös sopimuksia. Tilikirjan hajauttaminen useampaan paikkaan (siis kopioina) tekee siitä paremmin saatavilla olevan ja kestävämmän esim. kyberhyökkäyksiä kohtaan.

Tilikirjojen pitää kuitenkin olla yhtäpitäviä, joten niiden synkronointi on tärkeää. Synkronointia voidaan tehdä monin tekniikoin. Jos halutaan hyvin dynaamista, avointa ja globaalia järjestelmää, lohkoketjut konsensusprotokollineen ovat hyvä valinta tähän. Dynaamisimmat lohkoketjut muodostuvat kuitenkin helposti raskaiksi ja vaikeiksi hallita keskitetysti, mitä useimmat organisaatiot kuitenkin toivovat.

Hajautetut tilikirjat (DLT) ovatkin liiketoiminnan kannalta tärkeämpi käsite kuin lohkoketjut. Esimerkiksi suunnitellut nk. digitaaliset valuutat perustuvat useimmiten hajautettujen tilikirjojen toiminnallisuuteen, mutta harvemmin lohkoketjutoteutuksiin. DLT:n etuihin kuuluu toimintavarmuuden lisäksi myös pullonkaulojen vähentämisestä ja transaktioiden nopeudesta johtuva tehokkuus, monien liiketoimintaprosessien automatisointi, ja tarkasta kirjaamisesta seuraava äpinäkyvyys ja toiminnan seuraamisen ja

mittaamismahdollisuuksien parantuminen.

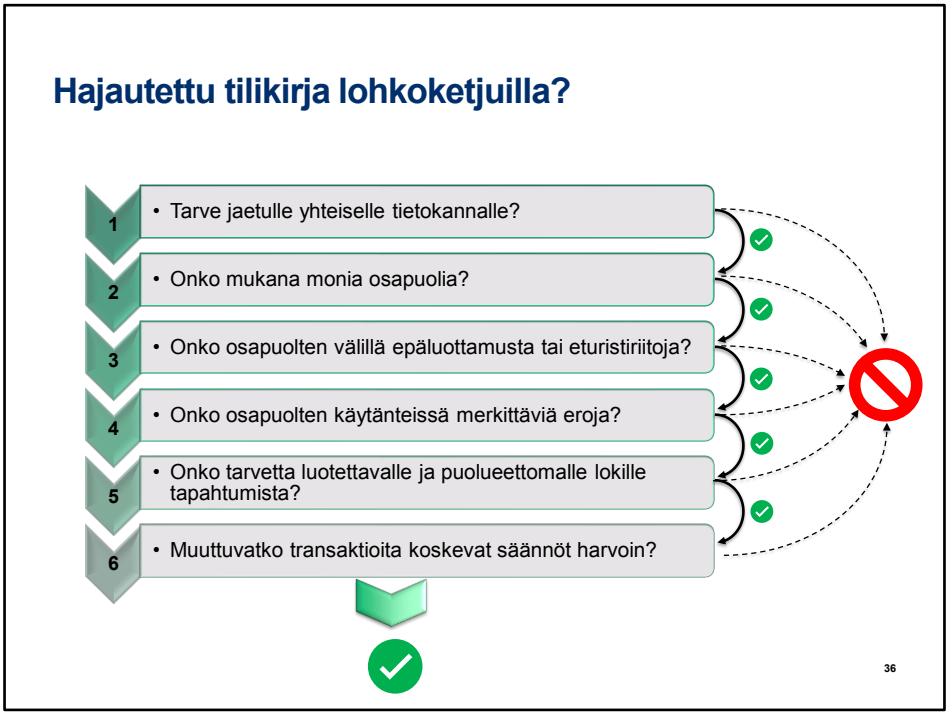
Jos voidaan kohtuudella taata, että tilikirjan eri kopiot pysyvät organisaation sisäisessä verkossa, ja kaikkien organisaation osien ei tarvitse nähdä kaikkien osien toimintaa, paljon tehokkaampiakin tekniikoita löytyy, kuten esimerkiksi Hyperledger-tyyliset ratkaisut, joita suunnitellaan jopa joihinkin digitaalisiin valuuttoihin pohjateknologiaksi.

Hajautettujen tilikirjojen käyttö

- **Hajautettujen tilikirjojen käytön edellytyksiä:**
  - Datan tuottajien moninaisuus ja keskinäinen epäluottamus
  - Infrastruktuurin hajauttaminen
  - DLT-teknologian pääsynhallintapolitiikan tuntemus ja käyttö
  - Datan siivoaminen
  - Liiketoimintaprosessien DLT-parametrien mittaaminen
  - Yhteensopivuusnäkökohdat
  - Compliance

  - *Koulutus!*

35



Jos organisaatio on päättänyt käyttää hajautettuja tilikirjoja ylipäätään, seuraava päätöspiste on sen jälkeen DLT:n toteuttaminen lohkoketjuilla vs. muilla tekniikoilla. DLT:n toteuttaminen lohkoketjuilla on raskaahkoa, joten tälle on hyvä olla olemassa painavat perusteet. Joissakin tapauksissa, esimerkiksi vakioidussa toiminnassa riippumattomien organisaatioiden välillä luottamuksen synnyttäminen muilla tavoin voi kuitenkin olla vaikeaa.

Lohkoketjujen kyberturvallisuus

- **Pääasiassa kohteena kryptovaluutat ja niiden käyttö:**
  - Kryptovaluutan vaihtopisteen hakkerointi
  - Kryptovaluuttalompakko-sovellusten hakkerointi
  - Käyttäjien yksityisten avainten / salasanojen kalastelu
  - Kryptovaluuttaoperaattorien kiristäminen (DDoS/Ransomware)
- **Tyypillisiä kyberhyökkäystekniikoita**
  - Kalastelu
  - Appien haavoittuvuudet
  - Smart contract – haavoittuvuudet (DeFi)
  - Pienten lohkoketjujen enemmistöosuuden kaappaaminen
  - Petolliset kryptovaluutan vaihtotoimijat

37

Mt. Gox on ehkä varhaisin ja kuuluisin esimerkki kryptovaluuttavaihtajan hakkeroinnista: yhteensä 850 000 bitcoinia varastettiin eri tahoilta. Mt Gox joutui konkurssiin.

Käyttäjien rajapinta kryptovaluuttoihin on yleensä erillisen sovelluksen kautta, joka hallinnoi käyttäjän salasanoja ja avaimia itse lohkoketjuihin. Näitä salasanoja ja appeja voidaan kalastella, varastaa ja hakkeroida siinä, kuin muitakin sovelluksia.

Lohkoketjukohtaisia haavoittuvuuksia on erityisesti PoW- ja PoS-tyyppisissä toteutuksissa enemmistöosuuden kaappaaminen: PoW- ja PoS-tyyppisten lohkoketjujen lähtöoletus on, että mikään yksittäinen toimija ei voi olla isompi kuin puolet koko lohkoketjun käyttäjäkunnasta. Mitattuna joko lohkoketjun omin assetein tai laskentatehossa. Jos lohkoketju on vasta käynnistymässä, tämä oletus ei usein päde. MonaCoin, ZenCash ja Verge on kaapattu esimerkiksi tällä tavoin.

Edistyneempien lohkoketjujen nk. Smart Contract-ominaisuus (eli esimerkiksi toimitussopimusten toteuttaminen automaattisesti lohkoketjun avulla) tarjoaa myös huolimattomasti toteutettuna hyökkäysvektoreita: Älysopimukset tulee

voida kuvata näiden omalla kuvauskielellä riittävän tarkasti, että sopimuksen määrittelyyn ei pääse porsaanreikiä. Lisäksi itse DeFi-vertaisverkkojärjestelmä, jota kautta älysopimuksia voidaan välittää, sisältää puutteita esimerkiksi varojen lähteen luotettavuuden tarkastamiseksi: transaction synnyttämisen ajankohdalla varat näyttävät olevan olemassa, mutta eivät enää sopimuksen täyttämisen ajankohtana.

Näistä älysopimusten käyttö on tämän kurssin toimialoille yleispätevin ja merkityksellisin suojattava kohde, sikäli kuin niitä toimitusketjun hallinnassa käytetään.

Hajautettujen tilikirjojen riskienhallinta

Johtaminen

DLT:t vastuu ylimmällä johdolla

DLT:t osaksi organisaation riskienhallintaa

Sovellusten suunnittelu ja kehittäminen

Oikean DLT-teknologian valinta

Älysopimusten hallinnan kehikot ja riskienhallinta

DLT:n compliance (erit. maksuliikenteessä)

Toimitusketjun riskienhallinta (esim. DLT-toimittajat ja operaattorit)

Yhteensopivuuden varmistaminen

Jatkuva valvonta ja ylläpito

Kyberturvallisuus

Avaintenhallinta

Datan yksityisyys

Liiketoiminnan jatkuvuuden hallinta

ERC3643